



Monday, March 23, 2026

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next.

Trojanization is the deliberate engineering of deception through appearance. It operates by disguising danger as opportunity, and by embedding concealed intent within symbols of safety, utility, or authority.



It does not storm the gates. It turns familiarity into camouflage, and trust into an attack surface. The target does not experience intrusion, it experiences reassurance and opportunity.

In the emotional domain, we have **emotional trojanization**. Romance scams are a classic form of trojanization. They follow the same structural logic. The **container** is affection. The **concealed payload** is exploitation. A romance scam is the embedding of predatory intent inside intimacy. Emotional attachment becomes the access mechanism. Trust is engineered, in order to be weaponized.

In **espionage**, trojanization is foundational. It often takes the form of embedding concealed strategic intent inside structures that appear ordinary, cooperative, or beneficial. For example, a commercial enterprise that operates as a front for intelligence collection, an academic exchange program that doubles as a recruitment pipeline, a cultural organization that quietly advances influence objectives, or a business partnership that enables access to sensitive technology.

The mechanism remains the same as in software or romance fraud. Legitimacy is constructed in order to be weaponized.

In [psychology](#), trojanization is the cognitive strategy in which harmful intent is concealed within signals of safety, familiarity, or attachment. Aggression activates defensive mechanisms. Trojanization is penetration through reassurance.

From a [cognitive perspective](#), trojanization exploits heuristic processing. Human beings rely on rapid evaluative shortcuts to determine safety and credibility. Signals such as warmth, similarity, authority, competence, or shared identity activate affiliative responses and reduce critical scrutiny. When a manipulative actor intentionally adopts these signals while concealing exploitative intent, they create a dissociation between perceived and actual threat.

[Attachment theory](#) provides a useful framework for understanding this dynamic. Attachment bonds are designed to create emotional security and proximity. They reduce anxiety and foster openness. In a trojanized psychological relationship, the external markers of attachment (empathy, attentiveness, validation, intimacy) are performed or simulated in order to generate emotional dependence. The target experiences increasing psychological safety, which in turn lowers boundaries and heightens self disclosure.

Through [mirroring](#), the manipulator reflects the target's values, preferences, vulnerabilities, and aspirations. This creates perceived similarity and accelerates relational bonding. The target interprets the interaction as authentic resonance. In reality, the resonance can be instrumental. The relational field becomes a container for concealed intent.

In [neuropsychology](#), positive social feedback activates dopaminergic pathways associated with bonding and reinforcement. The individual **wants to preserve** the coherence of the trusted narrative. This can delay recognition of manipulation, even when warning signs emerge. The psychological investment in the perceived relationship becomes self protective.

From a defensive standpoint, trojanization is [difficult to detect](#) because it weaponizes adaptive social mechanisms. Trust, attachment, empathy, and affiliation are foundational elements of human social functioning. Trojanization is the deliberate corruption of these mechanisms for strategic gain.

And so we return, inevitably, to [Troy](#). According to the myth, the Trojans stood before a big wooden horse and debated what to do. Some warned against bringing it inside the walls. Others argued it was a gift, a symbol of victory, perhaps even an offering of peace. We know how that deliberation ended.

Did something like that happen? Whether the events occurred exactly as told is a matter for historians and archaeologists. But [psychologically, the myth has endured](#) because it captures something enduring about human cognition.

We are inclined to trust what appears generous. We are reassured by symbols of legitimacy. We prefer the narrative of gift over the narrative of threat.

The city of Troy may have fallen once. The method, however, never did. It [migrated](#) from wooden horses to sealed letters, from forged identities to trojanized software, from staged affection to institutional fronts. The packaging changed, not the principle. History simply [kept upgrading the delivery system](#).

[In antiquity](#), it required carpentry. You needed timber, wheels, and a persuasive backstory. [By the Renaissance](#), a carefully sealed letter with the right crest could do the job. [In the twentieth century](#), a charming attaché with excellent manners and suspiciously broad research interests might suffice. [In the twenty-first](#), a polished PDF, a firmware update, or an app can accomplish what siege towers once attempted.

Each era believes it has [evolved beyond](#) the simplicity of Troy. We have compliance departments, encryption, background checks, antivirus software, and two factor authentication. Surely, we would not roll the horse inside the gates. But [the horse no longer looks like a horse](#). It looks like a partnership opportunity, a limited time upgrade a grant application, a job offer, or even love.

Yes, the method survived. It diversified, digitized, globalized, and learned excellent branding. The architecture remained the same, concealment within credibility, entry through trust.

The walls get taller. The defenses get smarter. And still, occasionally, someone says, [it's just a horse](#).

Best regards,



George Lekatis
President of the IARCP

Introducing an Advanced Specialization in Hybrid Risk and Resilience management, exclusively for CRCMPs.

We are thrilled to announce the launch of the Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program.

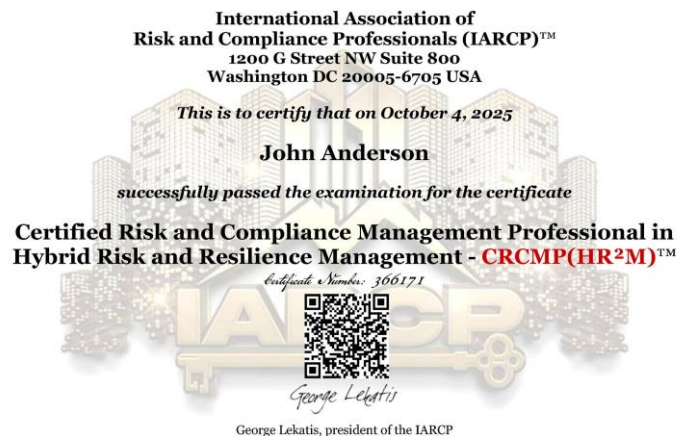
It builds on the solid foundation of the CRCMP designation and equips participants with cutting-edge knowledge to understand, identify, assess, and effectively manage complex hybrid risks.

The program prepares CRCMPs to strengthen organizational resilience across interconnected domains, including geopolitical and regulatory risk, counterintelligence, and supply chain resilience, while advancing capabilities in hybrid threat psychology, hybrid stress testing, and crisis management, ensuring readiness for an increasingly complex risk landscape.

Enrollment in the CRCMP(HR²M) program is restricted to professionals who have already passed the CRCMP exam. To preserve the credibility and value of this credential, the association does not allow substitutions, equivalency credits, or waivers of any kind. The curriculum assumes mastery of the CRCMP body of knowledge.

Learn more and view the full course synopsis:

https://www.risk-compliance-association.com/CRCMP_HR2M.htm



Number 1 (Page 7)

[Eurosystem Unveils Appia Roadmap for Europe's Tokenised Finance](#)



Number 2 (Page 9)

[The new financial ecosystem and the role of central banks](#)

Kazuo Ueda, Governor of the Bank of Japan, at the FIN/SUM 2026 "The new financial ecosystem shaped by AI and blockchain", Tokyo.



Number 3 (Page 13)

[Agencies clarify the capital treatment of tokenized securities](#)

Federal Deposit Insurance Corporation, Federal Reserve Board, Office of the Comptroller of the Currency



Number 4 (Page 15)

[SEC and CFTC Announce Historic Memorandum of Understanding Between Agencies](#)



Number 5 (Page 17)

[TRV Risk Monitor](#)

ESMA Report on Trends, Risks and Vulnerabilities No. 1, 2026



Number 6 (Page 20)

Scientists head underground to measure effects of gamma rays on superconducting qubits



Number 7 (Page 21)

Cybersecurity Regulations: Additional Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization



Number 8 (Page 25)

Printing Electronic Parts for Next-Generation Technologies
Custom inks and advanced printing methods enable durable transistors for smart devices



Number 9 (Page 28)

Global Law Enforcement Agencies, With Support From Meta, Disrupt Major Criminal Scam Networks Based in Southeast Asia



Number 10 (Page 30)

CISA Adds Three Known Exploited Vulnerabilities to Catalog



*Number 1***Eurosystem Unveils Appia Roadmap for Europe's Tokenised Finance**

- Appia will shape development of European tokenised financial ecosystem
- Central bank money to remain anchor of financial system amid digital transformation
- Appia sets out Eurosystem objectives and approach, expected to conclude in 2028

The Eurosystem published the roadmap for Appia, a strategic initiative to shape the development of a European tokenised financial ecosystem in which central bank money continues to play a central role. It will bring together the Eurosystem as well as public and private sector stakeholders, with the aim of building integrated, innovative and resilient tokenised wholesale financial markets in Europe.

“With Appia, we are building a road from today’s financial system to tomorrow’s tokenised markets, firmly grounded in central bank money,” said Piero Cipollone, member of the ECB’s Executive Board.

Tokenisation is the process of issuing or representing assets in the form of digital “tokens”, typically recorded on Distributed Ledger Technology (DLT) networks. For wholesale financial markets, tokenisation and DLT have the potential to improve efficiency by allowing multiple steps of an asset’s lifecycle – from issuance and trading to settlement, custody and servicing – to be bundled on a single platform. Moreover, tokenisation allows the deployment of smart contracts that enable a large range of innovative solutions.

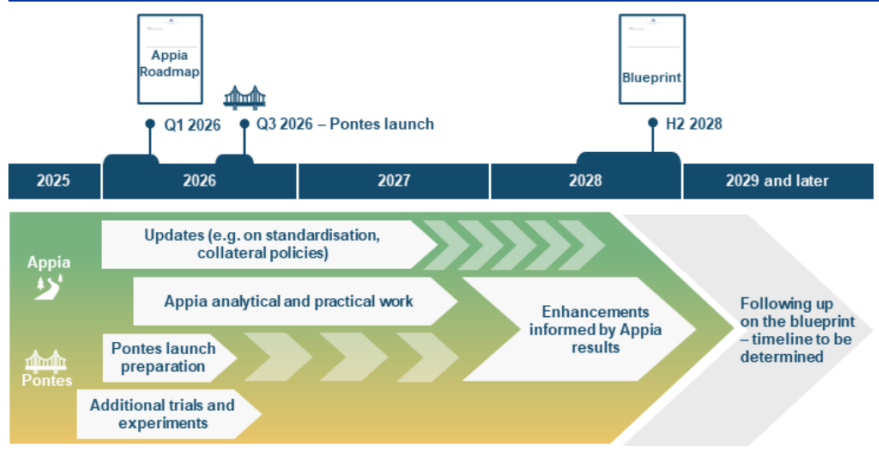
The Eurosystem’s strategy for providing tokenised wholesale central bank money rests on two complementary initiatives: Pontes and Appia. Pontes is the Eurosystem’s DLT solution that will be launched in the third quarter of 2026 to enable central bank money settlement for DLT-based transactions. Appia has a broader, longer-term perspective and will involve close cooperation with the market to explore how a wholesale financial ecosystem based on tokenisation and DLT could be designed.

The Eurosystem plans to crystallise its vision for this ecosystem in a blueprint to be published in 2028. In the meantime, the work under the Appia roadmap will inform and shape the delivery of tokenised market infrastructures and services both by the market and by the Eurosystem’s own Pontes offering, as it is gradually enhanced.

By preserving the role of central bank money as the anchor of the monetary system through Appia, the Eurosystem aims to ensure that monetary policy implementation remains effective, and that financial stability and the smooth

functioning of payment systems are safeguarded. The initiative seeks to foster a more integrated, competitive and innovative European payments and securities environment, strengthening Europe's strategic autonomy and resilience, and ensuring the euro's continued relevance as an international currency.

High-level timeline for Pontes and Appia



It will be developed in close cooperation with market participants, public sector bodies and academia. The Eurosystem invites feedback from stakeholders and expressions of interest in contributing to the forthcoming analytical and practical work. A feedback questionnaire is published alongside the Appia roadmap.

Appia builds on the Eurosystem's 2024 exploratory work on new technologies for wholesale central bank money settlement and marks a key step in translating experimentation into a concrete long-term strategy.

Appia will investigate different configurations for DLT networks that could serve as basic infrastructures for wholesale financial services. Shared infrastructures based on common standards could help reduce fragmentation, lower barriers to entry and support competition and innovation across Europe's financial markets.

The analysis will consider technological, market-driven and broader economic and geopolitical factors, including the trade-offs between single shared networks and multiple interconnected networks. Ensuring common standards and European governance will be a key objective.

To learn more:

<https://www.ecb.europa.eu/press/pr/date/2026/html/ecb.pr260311~14ddf51a77.en.html>

Roadmap:

<https://www.ecb.europa.eu/press/payments-news/ecb.pubconpm202603.en.html>

Number 2

[The new financial ecosystem and the role of central banks](#)

Kazuo Ueda, Governor of the Bank of Japan, at the FIN/SUM 2026 "The new financial ecosystem shaped by AI and blockchain", Tokyo.



Introduction

I am delighted to be given this opportunity to speak to you at the FIN/SUM 2026.

The year 2016, when the first FIN/SUM was held, marked a milestone for the Bank of Japan as well: we established the FinTech Center that very year, taking into account the growing momentum in fintech efforts and our support for these developments as the central bank such that they would contribute to enhancing financial services and ultimately achieving sustainable growth in Japan's economy.

The theme of this year's FIN/SUM is "The New Financial Ecosystem Shaped by AI and Blockchain." AI and blockchain have been significant topics of interest at the Bank since its founding of the FinTech Center.

Assuming application of these technologies in the areas of finance and payments, the FinTech Center conducted joint research with the European Central Bank (ECB), identifying opportunities and possible challenges that blockchain could bring to financial market infrastructures.

The Bank's Institute for Monetary and Economic Studies (IMES) also held workshops to explore legal considerations surrounding issues such as the use of distributed ledger technology (DLT) in securities settlements and the use of algorithms and AI.

Fast forward 10 years, blockchain technology has entered the implementation phase in a wide range of financial services. Coupled with the rapid advancement of generative AI, these developments have paved the way for innovative moves to create a financial ecosystem for a new era. In this vein, today I would like to talk about the role of central banks in this new financial ecosystem.

AI and Blockchain: Prospects for a New Financial Ecosystem

Taking a look at blockchain technology, a notable characteristic of decentralized finance, or so-called DeFi, is its high programmability. Specifically, DeFi is capable of deploying a system where smart contracts are utilized, enabling multiple transactions along the transaction chain, such as the borrowing and repayment of assets, to be bundled into a single transaction.

Efforts are also being made to develop a mechanism where payment transactions among multiple financial institutions, which result from cross-border payments, can be completed synchronously.

Early use cases to date include arbitrage transactions related to crypto assets and collateral exchange as well as the refinancing of lending conditions. Going forward, blockchain technology has the potential to develop as an infrastructure for transactions and settlements involving a wide range of assets and services, including delivery versus payment (DvP).

Shifting our focus to AI, which has proliferated rapidly over the past few years, this technology enables the analysis and processing of a variety of big data, whether it be with speed and precision or by taking an unconventional approach.

It is hoped that integrating AI and blockchain will allow the provision of enhanced financial services that utilize transaction and settlement data accumulated on the blockchain.

Examples of this include provision of financial advisory services via an AI agent, automation of value assessments and substitutions of collateral, as well as effective anti-money laundering and combating the financing of terrorism (AML/CFT) through detection of transactions that deviate from previously observed transactional patterns.

In order for the financial ecosystem of a new era -- characterized by new financial services being generated through the integration of AI and blockchain -- to develop, it is necessary to build a mechanism that ensures the transparency and authenticity of transactions, in particular the safety and robustness of payments, in accordance with the extent of system expansion and effects on economic society.

For the time being, the coexistence of multiple systems employing blockchains and a more conventional system is expected. It is necessary to consider the possibility that, while settlements are conducted smoothly within the individual systems, the same cannot be said for the conversion of payment instruments among different systems -- in other words, a lack of interoperability -- as well as the challenges that come with this.

1. This mechanism, which enables atomic transactions, refers to an all-or-nothing process where each relevant transaction is either executed completely or not executed at all.
2. Atomic transactions are also relevant to Project Agorá, as discussed later. Participants are engaging in efforts to develop a mechanism where payment transactions among multiple financial institutions, which result from cross-border payments, can be completed through atomic transactions by utilizing smart contracts and blockchains.
3. For details on the utilization of blockchain in finance, see Ueda, K., "Future of Payments and the Role of Central Banks," speech at the Symposium for

the 40th Anniversary of the Center for Financial Industry Information Systems (FISC), December 4, 2024.

4. Meanwhile, new methods of analysis such as nowcasting have emerged. Specifically, generative AI is utilized to sort, by type of goods, large volumes of price data collected from markets, which allows users to generate real-time price indices and gain an accurate grasp of inflationary developments.

The Role of Central Banks: As an Anchor of Trust

In addition to achieving price stability, many central banks, in their capacity, are expected to provide central bank money such as cash and central bank current account deposits -- the payment instrument supporting economic activity -- while safeguarding payment stability.

When making payments today, bank deposits and a wide array of cashless payment instruments are used besides cash. Underlying this coexistence of the various payment instruments is not only a framework ensuring the soundness of each of these payment instruments but also central bank money, which acts as a bridge among the various payment instruments.

Central bank money provides a foundation where money can be exchanged at par value for all payment instruments; in other words, the singleness of money is secured.

Unless the deposits at different banks are connected through central bank deposits, there is a risk that people will perceive this as variation in the value of deposits among banks, as was the case during the wildcat banking era in 19th-century United States. This would bring about negative effects on payments and general economic activity.

Central bank money also plays a role in large-value payments: as the safest and most liquid settlement asset, it contributes to the containment of systemic risk in, for example, interbank funds settlement and securities settlement among financial institutions.

Central bank money therefore fulfils its role as the anchor of trust for an economy by serving as the foundation that connects all payment instruments and by functioning as the safest and most liquid settlement asset.

Let us turn to prospects regarding the development of the anchor of trust in a new financial ecosystem. A number of scenarios can be envisaged.

By providing a mechanism where payment instruments on various blockchains -- different payment instruments in some cases -- can carry out a smooth exchange through the use of central bank money, this would ensure interoperability achieved by using central bank money as the medium of exchange.

Alternatively, it is also plausible to secure and provide a mechanism under which transactions of assets on blockchains are settled with central bank money. This could be achieved by either settling assets with tokenized central bank money on the blockchain or by connecting the existing system for central bank money with a new system for transactions on the blockchain.

A wide range of experimental projects are in progress across the globe to delve into these ideas I have just raised. When proceeding with such projects, exploring unintended consequences is just as important as exploring the plausible effects. For example, smart contracts are highly convenient in that they allow transactions to be carried out automatically without any manual labor.

When the design of the smart contracts is inadequate, however, there is a risk that the stability of financial markets and payment systems will be threatened due to fraudulent use. In areas where technological advancement is occurring at considerable speed and direct regulation is not the optimal approach, best practices may be explored to ensure the safety of payments through international discussions with participants including central banks.

In order for a central bank to effectively employ new technologies in enhancing a mechanism under which to provide an anchor of trust, it is essential to carry out thorough institutional arrangements that take into account use cases and the nature of transactions as well as the risks involved. For this reason and more, it is crucial for central banks to gain deep insights into these new technologies.

To learn more:

https://www.boj.or.jp/en/about/press/koen_2026/ko260303a.htm



*Number 3***Agencies clarify the capital treatment of tokenized securities**

Federal Deposit Insurance Corporation, Federal Reserve Board, Office of the Comptroller of the Currency



The federal bank regulatory agencies today jointly issued answers to frequently asked questions to clarify the capital treatment of tokenized securities.

A security is often referred to as "**tokenized**" when ownership rights in the security are represented using distributed ledger technology. The answers to the frequently asked questions clarify that an eligible tokenized security should generally receive the same capital treatment as the non-tokenized form of the security under the capital rule. The agencies also clarified that the capital rule is technology neutral, and the technologies used to issue and transact in a security do not generally impact its capital treatment.

As with any exposure, banks holding tokenized securities must apply sound risk management practices and comply with applicable laws and regulations.

What is the capital treatment for eligible tokenized securities?

- The capital rule for banking organizations implemented by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (together, the federal banking agencies) is technology neutral. The technologies used to issue and transact in a security do not generally impact its capital treatment.
- Accordingly, an eligible tokenized security should be treated in the same manner as the non-tokenized form of the security would be treated under the capital rule. Similarly, a derivative that references an eligible tokenized security should be treated for capital purposes as a derivative that references the non-tokenized form of the security.
- As with any exposure, banking organizations holding tokenized securities must apply sound risk-management practices and comply with applicable regulations.

Would a tokenized security qualify as financial collateral for purposes of the capital rule?

The technologies used to confer legal rights to a security do not impact its ability to meet the definition of "financial collateral" in the capital rule. A banking

organization should evaluate the tokenized security according to the definition of "financial collateral" in the capital rule.

An eligible tokenized security that satisfies the definition of "financial collateral" would qualify as financial collateral for purposes of the capital rule and may be recognized by the banking organization as a credit risk mitigant if all the other relevant requirements in the capital rule are met.

As financial collateral, an eligible tokenized security would be subject to the same haircuts applicable to the non-tokenized form of the security.

To learn more:

<https://www.federalreserve.gov/newsevents/pressreleases/bcreg20260305a.htm>



*Number 4***SEC and CFTC Announce Historic Memorandum of Understanding Between Agencies**

The Securities and Exchange Commission and the Commodity Futures Trading Commission today announced that they have entered into a Memorandum of Understanding (MOU) to guide coordination and collaboration between the two agencies to support lawful innovation, uphold market integrity, and ensure investor and customer protection.

The MOU reflects both agencies' commitment to provide fair notice to market participants, respect individual liberty, and foster lawful innovation with the minimum effective dose of regulation to enhance U.S. competitiveness in finance.

“For decades, regulatory turf wars, duplicative agency registrations, and different sets of regulations between the SEC and CFTC have stifled innovation and pushed market participants to other jurisdictions,” said SEC Chairman Paul S. Atkins. “This updated Memorandum of Understanding will serve as a roadmap for a new era of harmonization between the agencies – one that is critical to support U.S. leadership in this next chapter of financial innovation. By aligning regulatory definitions, coordinating oversight, and facilitating seamless, secure data sharing between agencies, we will ensure our rules and regulations deliver the clarity market participants deserve.”

“America’s financial markets are the envy of the world because they scale and adapt to meet investor demands. Like our markets, the CFTC’s and SEC’s regulatory frameworks must also evolve and modernize to accommodate the needs of our market participants,” said CFTC Chairman Michael S. Selig. “This Memorandum of Understanding solidifies the agencies’ commitment to harmonize regulatory frameworks to provide comprehensive and seamless financial market oversight. By working together, we’ll eliminate duplicative, burdensome rules and close gaps in regulation for the benefit of all Americans and usher in a Golden Age of American finance.”

In conjunction with the MOU, the agencies created a Joint Harmonization Initiative to advance coordinated oversight and promote regulatory clarity in areas of common regulatory interest. The initiative will support coordination across the policymaking, examination and enforcement functions of each agency, particularly for joint applications and shared policy efforts, including:

- Clarifying product definitions through joint interpretations and rulemakings.
- Modernizing clearing, margin, and collateral frameworks.

- Reducing frictions for dually registered exchanges, trading venues, and intermediaries.
- Providing a fit-for-purpose regulatory framework for crypto assets and other emerging technologies.
- Streamlining regulatory reporting for trade data, funds, and intermediaries.
- Coordinating cross-market examinations, economic analyses, risk monitoring, surveillance, and enforcement.

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE U.S. SECURITIES AND EXCHANGE COMMISSION
AND
THE U.S. COMMODITY FUTURES TRADING COMMISSION
REGARDING
HARMONIZATION IN AREAS OF COMMON REGULATORY INTEREST

The mission of the SEC is to protect investors, maintain fair, orderly, and efficient securities markets, and facilitate capital formation. The mission of the CFTC is to promote the integrity, resilience, and vibrancy of the U.S. derivatives markets through sound, principles-based regulation. In an increasingly convergent financial ecosystem, the SEC and CFTC (the “Parties”) share significant areas of common regulatory interest, including oversight of trading venues, clearinghouses, data repositories, pooled investment vehicles, dealers and other intermediaries, and products that span securities and derivatives frameworks.

To learn more:

<https://www.sec.gov/newsroom/press-releases/2026-26-sec-cftc-announce-historic-memorandum-understanding-between-agencies>

Memorandum: <https://www.sec.gov/files/mou-sec-cftc-2026.pdf>



Note for Number 5

The term “hybrid threats” now appears explicitly in the European Securities and Markets Authority (ESMA) risk monitor. ESMA states: “Cyber and hybrid threats remained elevated, increasing the risk of severe disruptions to market infrastructure and amplifying systemic vulnerabilities.”

ESMA links hybrid threats to operational and technology disruptions in financial markets. This is significant because it shows that EU financial supervision is adopting the hybrid threats vocabulary used in security and defense policy.

Number 5

TRV Risk Monitor

ESMA Report on Trends, Risks and Vulnerabilities No. 1, 2026



Risk summary

In the second half of 2025 and into early 2026, equity valuations reached record highs, underscoring mounting risks of unsustainable pricing and disorderly corrections that could reverberate across markets, even after a modest subsequent retreat.

The October crypto flash crash dampened exuberance in crypto markets, yet valuations remain at elevated levels. Private credit emerged as a systemic vulnerability following US defaults highlighting opacity and systemic interlinkages.

Debt sustainability concerns grew in both the EU and U.S. on the back of rising public deficits.

Cyber and hybrid threats remained elevated, increasing the risk of severe disruptions to market infrastructure and amplifying systemic vulnerabilities.

These market developments collectively contributed to keep risks of market and systemic stress elevated, particularly given the backdrop of evolving geopolitics and continuing uncertainty.

Asset price correlations have also increased since April, indicating enhanced contagion risk between asset classes. In light of this assessment, we continue to score market, contagion and operational risk categories at the highest level, credit risk at high and environmental risk at medium level.

Stretched valuation levels, which exacerbate the risk of a sharp correction in a volatile environment, explain the high-risk score for securities markets and crypto assets.

Risk outlook

Persistent uncertainty continues to cloud the outlook, with stretched global equity valuations posing significant risks of abrupt corrections and systemic contagion and credit quality potentially deteriorating.

Tariff-driven inflation may complicate central bank policy decisions, with potential for volatility in bond and currency markets. The rapid expansion of private credit adds leverage and liquidity vulnerabilities, where setbacks could cascade into wider financial distress.

Growing interlinkages between crypto and traditional markets, including through stablecoins, warrant close attention too, as they increase potential negative spillovers.

In addition, cyber and hybrid threats represent an escalating concern. Retail and institutional investors should remain vigilant and maintain robust liquidity buffers to withstand sharp market corrections.

Risk indicators

Risk categories

	Previous risk level	Current risk level	Outlook
Liquidity	■	■	→
Market	■	■	→
Credit	■	■	→
Contagion	■	■	→
Operational	■	■	→
Environmental	■	■	→

Market segments

	Previous risk level	Current risk level	Outlook
Securities markets and crypto-assets	■	■	→
Infrastructures, services	■	■	↗
Asset management	■	■	→
Retail investors	■	■	→

Note: Assessment of the main risks by drivers and categories for markets within ESMA's remit since the last assessment, and outlook for the forthcoming quarter. Risk dashboard based on the categorisation of the European Supervisory Authorities Joint Committee. Risk drivers are key factors influencing potential risks within ESMA's remit, assessed through a narrative-based approach. Colours indicate current risk intensity. Coding: green = potential risk; yellow = elevated risk; orange = high risk; red = very high risk. Upward-pointing arrows = increase in risk intensity; downward-pointing arrows = decrease in risk intensity; horizontal arrows = no change. Change is measured with respect to the previous period; the outlook refers to the forthcoming period.

Risk drivers

Financial stability and orderly markets

Outlook Geopolitical and macroeconomic uncertainties: Ongoing geopolitical uncertainties, including on regional conflicts and in global trade, increase fragmentation risk and could be a trigger for event risk and large, sudden and potentially lasting price movements.

The EU's economic performance also provides an uncertain backdrop for EU financial markets, especially given the expected impact of higher tariffs.

Rising public and private debt is set to increase debt servicing, which will continue to weigh on issuers. Persisting elevated equity market valuations, linked to technology and AI in the US and financials in the EU, further intensify risks of sharp market corrections in a context of increasing market reactivity and volatility.

Operational and technology disruptions: Recent incident data show that the financial sector is increasingly targeted by cyber and hybrid threats, while critical infrastructures and service providers remain vulnerable to operational dependencies that can propagate shocks across participants and markets.

Efforts to strengthen operational-resilience frameworks, enhance third-party oversight and improve incident reporting and testing are central to mitigating the potential financial-stability and orderly-market impact of future disruptions.

TRV Risk Monitor

ESMA Report on Trends, Risks and Vulnerabilities

No. 1, 2026



To learn more:

https://www.esma.europa.eu/sites/default/files/2026-03/ESMA50-1949966494-4041_TRV_Risk_Monitor_1_2026.pdf



Number 6

Scientists head underground to measure effects of gamma rays on superconducting qubits



In a pioneering study at an underground laboratory at Fermilab, scientists measured bursts of charge across multiple superconducting qubits. Their work advances understanding of how background noise impacts qubits while contributing to the development of more precise sensors to discover new physics phenomena and more fault-tolerant [quantum computers](#).

Beneath Earth's surface, shielded from the effects of most cosmic rays, is the Northwestern Experimental Underground Site, or NEXUS. Located about 350 feet underground at Fermi National Accelerator Laboratory, the research facility enables scientists to study the behavior of quantum devices in their quest to find evidence of dark matter.

It's here that a multi-institutional team of scientists took measurements of correlated charge noise in a chip comprised of multiple superconducting qubits for the first time.

Superconducting qubits are a leading option for building quantum computers. However, they are sensitive to disturbances from their environment and can make errors. By understanding how electrical fluctuations called charge noise affect superconducting qubits, scientists can find ways to reduce these errors and improve quantum computers.

When an ionizing particle, like a cosmic ray or gamma ray passes through such a chip, it can create bursts of charge that can impact information stored in qubits. Scientists can directly measure these events because the qubits used in the study are incredibly sensitive to fluctuations in charge.

“Understanding whether a charge burst could affect multiple qubits as the charge moves through the chip — what researchers call correlated charge noise — is crucial to scientists who use quantum sensors to detect very faint signals that are possibly from dark matter, and to computer scientists, who are interested in correcting errors,” said Daniel Bowring, a scientist at Fermilab and organizer of this study.

To learn more:

<https://news.fnal.gov/2026/03/scientists-head-underground-to-measure-effects-of-gamma-rays-on-superconducting-qubits/>



*Number 7***Cybersecurity Regulations: Additional Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization**

441 G St. N.W.
Washington, DC 20548

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Our nation increasingly depends on computer-based information systems and electronic data to execute fundamental operations and to process, maintain, and report crucial information.

Further, nearly all federal and nonfederal operations, including the nation's critical infrastructure, are supported by these systems and data.

Consequently, the safety of these systems and data is critical to public confidence and the nation's security, economy, and welfare. GAO has identified cybersecurity as a government-wide high-risk area for more than 25 years.

Recognizing a growing threat, we first designated information security as a government-wide high-risk area in 1997.

Subsequently, in 2003, we expanded the information security high-risk area to include the cybersecurity of critical infrastructure.

We further expanded this high-risk area in 2015 to include protecting the privacy of personally identifiable information.

In our most recent update on this high-risk area in February 2025, we reiterated that fully establishing and implementing a national cybersecurity strategy was needed to protect the nation's information systems and infrastructure.

You asked us to convene a series of discussions with industry representatives to gather their perspectives on federal progress in harmonizing cybersecurity regulations, and to provide periodic updates on these discussions. Our first report in this series was issued in July 2025.

This is the second such report and summarizes the views shared by selected industry participants in a September 2025 panel.

Participants commented on the impact of federal cybersecurity regulations and federal agencies' progress, challenges, and opportunities in harmonizing these regulations. To gather these perspectives, GAO convened a panel discussion on September 17, 2025.

The panel included seven representatives, each from different critical infrastructure sectors: communications, energy, financial services, healthcare and public health, information technology, transportation systems, and water and wastewater systems.

The representatives included directors of information technology and cybersecurity, chief information officers, general counsel and regulatory affairs specialists.

We committed to treat industry participants' comments made during the panel with confidentiality to encourage them to speak candidly, unless they otherwise agreed to attribution in specific cases. The information in this report summarizes the industry participants' perspectives and the points that were raised.

The summary of panelists' viewpoints does not necessarily reflect a unanimous opinion of the panel or a collective view of the panelists' respective sectors. See enclosure I for additional information on our objectives, scope, and methodology. For a list of panel participants, see enclosure II.

We conducted our work from August 2025 to March 2026 in accordance with all applicable sections of GAO's Quality Assurance Framework. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work.

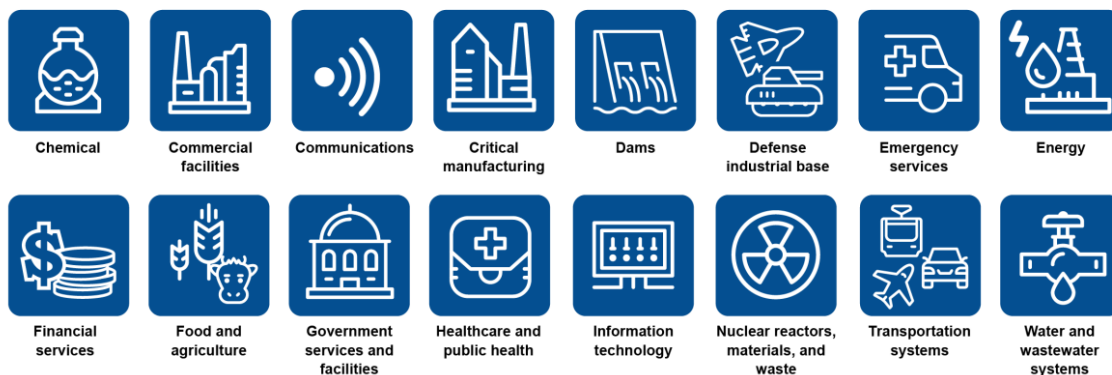
We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

Background

Cyber-based intrusions and attacks on both federal and nonfederal systems by malicious actors are becoming more common and disruptive.

These attacks threaten the continuity, confidence, integrity, and accountability of essential systems.

Figure 1: The 16 Critical Infrastructure Sectors



Sources: GAO analysis of National Security Memorandum-22; motorama/stock.adobe.com (icons). | GAO-26-108685

Moreover, the risks to these systems, including insider threats from witting or unwitting employees, mounting threats from around the globe, and the rise of new and more destructive attacks, collectively threaten to compromise sensitive data and destabilize critical operations.

Because the private sector owns most of the nation's critical infrastructure (see fig. 1), it is vital that the public and private sectors work together to protect these assets and systems.

Toward this end, various federal agencies are responsible for assisting the private sector in protecting critical infrastructure, including enhancing cybersecurity. In doing so, federal agencies have issued a variety of regulations to help protect the nation's critical infrastructure.

However, according to the Office of the National Cyber Director, when critical infrastructure sectors are subject to multiple cybersecurity regulations, the result can be conflicting guidance, inconsistencies, and redundancies.

Harmonization refers to the development and adoption of consistent standards and regulations. Such consistency is important when critical infrastructure sectors are subject to multiple cybersecurity regulations so that these requirements will not overlap, duplicate, or contradict each other.

In June 2024, we testified that consistent cybersecurity regulations could help protect against the increasing risks that threaten our nation's critical infrastructure sectors.

At that time, we also discussed the importance of harmonized regulations in avoiding adverse impacts, such as conflicting incident reporting requirements. We have previously identified concerns around varying federal cybersecurity requirements and the implementation of those requirements.

For example, in May 2020, we identified adverse impacts that varying cybersecurity requirements issued by selected federal agencies and related compliance assessments had on state government agencies.

We made recommendations to the five agencies to improve coordination with respect to their cybersecurity requirements and assessments of state government agencies. Of the 12 recommendations we made in this area, the agencies have implemented 11 and partially addressed the one remaining.

Further, in July 2024, we reported on the Department of Homeland Security's efforts to implement federal cyber incident reporting requirements and the challenges with harmonizing these requirements. Though we did not have recommendations, we identified challenges including differences in the

- (1) definitions of reportable cyber incidents,
- (2) timelines and triggers for when reports must be made,
- (3) contents of cyber incident reports, and
- (4) how the reports are submitted to federal agencies.

Enclosure II: Panel Participation

We convened a 3-hour panel of industry participants from multiple critical infrastructure sectors, selected randomly from public comments on a proposed rule for CIRCIA implementation and a request for information from the Office of the National Cyber Director on views regarding cyber regulatory harmonization. The panel was held virtually on September 17, 2025. The seven industry participants who attended the panel and represented different critical infrastructure sectors are listed below.

Tara Hairston	Alliance for Automotive Innovation (transportation systems)
Stephanie Kiel	Google LLC (information technology)
Andrew Morris	America's Credit Unions (financial services)
Loretta Polk	NCTA - The Internet & Television Association (communications)
Dave Roberts	AlexRenew (water and wastewater systems)
Dr. Steven Waldren	American Academy of Family Physicians (healthcare and public health)
Bill Zuretti	Electric Power Supply Association (energy)

To learn more: <https://www.gao.gov/assets/gao-26-108685.pdf>



Number 8

Printing Electronic Parts for Next-Generation Technologies Custom inks and advanced printing methods enable durable transistors for smart devices



Tiny electronic devices, called microelectronics, may one day be printed as easily as words on a page, thanks to new research from scientists at the U.S. Department of Energy's (DOE) Argonne National Laboratory.

Building on years of progress in printed electronics, the team has shown how to create durable, low-power electronic switches, called transistors, by combining custom inks and a specialized printing process.

These switches, which control the flow of electrical current to turn circuits on and off, use very little power, are built to last and show new behaviors not seen in earlier printed devices. This research could help create flexible sensors, smart windows and other new technologies that need reliable, energy-saving electronics.

The scientists used a method called aerosol jet printing, which works like an inkjet printer. But instead of regular ink, it uses specially formulated ink made from nanoparticles. The printer turns the ink into a fine mist and sprays it onto a surface, building up layers to form electronic parts.

Unlike traditional manufacturing, which often requires expensive equipment and high temperatures, aerosol jet printing works at lower temperatures and can print on flexible or even 3D surfaces. This approach makes it easier and faster to develop and test new electronic designs.

To fine-tune these inks, the team used the Center for Nanoscale Materials (CNM) at Argonne, to watch how nanoparticles clump together, see how they change with heat and check the stability and makeup of the dried films — insights that helped improve the ink formulations.

They also used the 2-ID-E hard X-ray microprobe at Argonne's Advanced Photon Source (APS), to map the shape and elemental makeup of the printed devices, complementing high-resolution X-ray spectroscopy studies at Brookhaven's National Synchrotron Light Source II (NSLS-II). CNM, APS and NSLS-II are all DOE Office of Science user facilities.

A key ingredient in these printed devices is vanadium dioxide. This material is special because it can act like a wire, letting electricity flow, or like an insulator, blocking electricity. This switching ability is important for making electronic circuits and memory devices, which store and process information.

To control the flow of electricity in the transistors, the team used a process called redox gating. In simple terms, this means they use a chemical reaction to add or remove electrons from the vanadium dioxide. By applying a small voltage — less

than what is used in a typical battery — they can turn the transistor on or off. This method is less harsh than other techniques, which could damage the material and make devices wear out quickly.

In laboratory tests, the printed transistors operated at voltages as low as 0.4 to 0.5 volts and kept working for more than 6,000 on-off cycles, which is much longer than previous printed devices. The switches also responded quickly, changing states in about one second.

“We chose printing methods for two main reasons,” said Argonne Materials Scientist Yuepeng Zhang. “First, printing enables rapid prototyping and iterative design, which helps us optimize materials and device structures quickly. Second, printed electronics have benefits for device functionality, especially since our devices show a well-modulated current response to voltage, making them suitable for printed logic devices and niche applications.”

When the printed transistor was switched on using a small control signal of 0.5 volts, it allowed about 50% more electricity to flow through it compared to when it was off. In other words, the device could boost the flow of electric current by half with just a tiny amount of power. This shows that the transistor can reliably control electricity using very little energy, which is important for making low-power and flexible electronic devices.

Wei Chen, a chemist from Argonne and the University of Chicago, emphasized the durability of the new devices. “Redox gating is robust and does not damage the materials, so we can run thousands of cycles without issues,” he said. “In previous methods, devices could only run a few times — sometimes just 10 cycles — before failing. Our devices can run thousands of cycles with no problem.”

Right now, these printed transistors are larger and slower than the tiny silicon chips found in most electronics. But this research shows that it is possible to make strong, low-power devices with printing methods.

Chen added, “From my perspective, the next step is logic devices. We’ve been in contact with industry partners interested in testing our devices for logic applications, which are the basic building blocks for computers. That is something I would like to pursue.”

They are also exploring how these printed devices could be used in neuromorphic computing, an area that mimics the way the human brain processes information.

To move printed electronics from the lab to real products, the researchers say more teamwork is needed between scientists and industry. They also believe that artificial intelligence and machine learning could help improve the printing process and make development faster.

“Printing involves many variables to adjust, and machine learning can help us find the best settings more quickly,” Zhang said.

With more research and collaboration, printed hybrid electronics could help make future technology more flexible, affordable and energy efficient.

The results of this research were published in *Advanced Materials Technology*.

Other contributors to this work include Samuel Miller and Hua Zhou from Argonne; and Evan Musterman, Andrew Kiss and Yang Yang from the National Synchrotron Light Source II at DOE's Brookhaven National Laboratory. Andrew Erwin and Shiyu Hu were at Argonne when this research is conducted.

This work was primarily supported by the Laboratory Directed Research and Development program at Argonne, with additional support from DOE's Office of Science, Basic Energy Sciences.

To learn more: <https://www.bnl.gov/newsroom/news.php?a=122857>



*Number 9***Global Law Enforcement Agencies, With Support From Meta, Disrupt Major Criminal Scam Networks Based in Southeast Asia***Takeaways*

- International law enforcement joined Meta, the Royal Thai Police, the FBI, and the DOJ Scam Center Strike Force to disrupt criminal scam centers in southeast Asia that targeted the United States, the United Kingdom, and countries across Asia and the Pacific region.
- Based on information shared by law enforcement partners, Meta disabled over **150,000 accounts** involved in or supporting scam center networks, and the Royal Thai Police Anti-Cyber Scam Center arrested 21 individuals for their involvement in scam activity.
- This was our second joint enforcement surge since December, demonstrating how global law enforcement continues to partner with Meta and peer companies to disrupt organized online crime and protect people from scams.

Online scams have become significantly more sophisticated and industrialized in recent years, with criminal networks often based in Southeast Asia in countries like Cambodia, Myanmar, and Laos running what amount to full-scale business operations.

These operations cause real harm — they upend lives, destroy trust, and are deliberately designed to avoid detection and disruption.

The work to protect people against scammers is never done, and requires ongoing collaboration with partners across the tech industry and law enforcement to ensure a safer experience for everyone online.

This collaboration is the driving force behind the second Joint Disruption Week in Bangkok, which was led last week by the Royal Thai Police Anti-Cyber Scam Center (ACSC), the FBI, the DOJ Scam Center Strike Force, and other law enforcement agencies that joined Meta from around the globe.

As a result of this operation and information shared by law enforcement partners, Meta investigators disabled over 150,000 accounts associated with scam centers. The effort also led to 21 arrests made by the Royal Thai Police.

This operation builds on the success of a Joint Disruption Week pilot program in December, during which the ACSC, in close collaboration with Meta, DOJ Scam Center Strike Force, FBI, Homeland Security Investigations, US Secret Service,

and other law enforcement agencies engaged in intensive live information sharing.

This resulted in the removal of 59,000 accounts, Pages, and Groups from Meta's platforms and six arrest warrants, demonstrating a powerful and replicable model for partnering with law enforcement to enforce against organized online crime.

For the second Joint Disruption, Meta, the ACSC and US law enforcement welcomed a broader coalition of partners from countries including the UK (National Crime Agency), Canada, Korea, Japan, Singapore, the Philippines, Australia, New Zealand, and Indonesia. Representatives from the messaging app LINE also joined to participate in discussions.

The goal was to once again share information but also to deepen partnerships, improve collective systems, and strengthen action against the criminal syndicates behind these scams. Throughout the week, partners shared insights that allowed them to connect the dots between disparate pieces of information.

To learn more:

<https://about.fb.com/news/2026/03/meta-global-law-enforcement-disrupt-major-southeast-asia-criminal-scam-networks/>



Number 10

CISA Adds Three Known Exploited Vulnerabilities to Catalog



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

- CVE-2021-22054 **Omnissa Workspace** ONE Server-Side Request Forgery
- CVE-2025-26399 **SolarWinds** Web Help Desk Deserialization of Untrusted Data Vulnerability
- CVE-2026-1603 **Ivanti** Endpoint Manager (EPM) Authentication Bypass Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the KEV Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise.

BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet for more information.

Although BOD 22-01 only applies to FCEB agencies, CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of KEV Catalog vulnerabilities as part of their vulnerability management practice. CISA will continue to add vulnerabilities to the catalog that meet the specified criteria.

To learn more:

<https://www.cisa.gov/news-events/alerts/2026/03/09/cisa-adds-three-known-exploited-vulnerabilities-catalog>



Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn pages of the Association.

Readers will make their own determination of how suitable the information is for their usage and intent. The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of interpretative;
- does not prejudice the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;
- does not prejudice the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.

General Terms and Conditions for all visitors:

<https://www.risk-compliance-association.com/Privacy.htm>

International Association of Risk and Compliance Professionals (IARCP)



The International Association of Risk and Compliance Professionals (IARCP) is a global community of experts working in risk and compliance management that explore career avenues and acquire lifelong skills. The IARCP is a business unit of Compliance LLC, a company incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training and certification in fifty-seven countries.

To learn more: <https://www.risk-compliance-association.com/Privacy.htm>

Our training and certification programs:

1. Certified Risk and Compliance Management Professional (CRCMP), distance learning and online certification program. You may visit: <https://www.risk-compliance-association.com/Distance Learning and Certification.htm>

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in fifty-seven countries. Companies and organizations around the world consider the CRCMP a preferred certificate.

You can find more about the demand for CRCMPs at: <https://www.risk-compliance-association.com/CRCMP Jobs Careers.pdf>

International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW, Suite 800, Washington, DC 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Discover 20 amazing CRCMP Jobs
(and what it takes to get hired)

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board
Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...

Senior Manager Vendor Risk Management
Ethical & Certified Family of Companies (Ethical) 5,133 members
New Brunswick, NJ

Ethics & Compliance Controlling Manager - North America
Nike
Beaverton, OR
A minimum of 5+ years of experience in risk management, accounting, auditing or related functions
Experience within a large, multi-national company and CRCMP, CFE or other certification preferred
Solid understanding of the technical aspects of the Control Practices Act, as well as local Anti-Bribery laws and regulations
In-depth understanding of crafting and implement while also possessing a strong documentation skills
Understanding of internal auditing standards, CO Control Framework, and risk assessment practices
Experience in planning, implementing and report assessment results

Risk Science Business Process Lead, Senior Associate
Capital One
Bethesda, MD
Ex: \$110,000 - \$145,000 a year
Lynn, GA; Sigma, MI; IBM, NY; or CRISC/CISSP/ISO 9001/1/19949, United States of America, Missouri, Virginia...

Application Security Advisor-Penetration Tester
CS&A - Staff Services, Inc.
Ex: \$105,000 - \$140,000 a year
Professional designation in CISSP, CISA, CRISC, CISM, CISM, GIAC, GISEP, OAWB, or CRCMP. Purpose of Job: IMPROVE...

GRC Solutions Architect
IBM
Houston, TX
IBM is looking for a GRC Solutions Architect to join our team in Houston, TX. The role will be responsible for designing, implementing, and maintaining GRC solutions for our clients. The role will also be responsible for providing technical support to our clients and for managing the GRC solutions architecture.

Ethics & Compliance Controlling Manager - North America
Nike
Beaverton, OR
A minimum of 5+ years of experience in risk management, accounting, auditing or related functions
Experience within a large, multi-national company and CRCMP, CFE or other certification preferred
Solid understanding of the technical aspects of the Control Practices Act, as well as local Anti-Bribery laws and regulations
In-depth understanding of crafting and implement while also possessing a strong documentation skills
Understanding of internal auditing standards, CO Control Framework, and risk assessment practices
Experience in planning, implementing and report assessment results

Senior Audit Specialist, Global Risk & Assurance
SAP
New York, NY
SAP is looking for a Senior Audit Specialist, Global Risk & Assurance to join our team in New York, NY. The role will be responsible for designing, implementing, and maintaining GRC solutions for our clients. The role will also be responsible for providing technical support to our clients and for managing the GRC solutions architecture.

CR and CR FCM Leader (Independent Testing Specialist)
Veeva
Cincinnati, OH
Veeva is looking for a CR and CR FCM Leader (Independent Testing Specialist) to join our team in Cincinnati, OH. The role will be responsible for designing, implementing, and maintaining GRC solutions for our clients. The role will also be responsible for providing technical support to our clients and for managing the GRC solutions architecture.

Lead Budgeting Testing Officer - Commercial Banking (Independent)
Wells Fargo Bank
Charlotte, NC
Wells Fargo Bank is looking for a Lead Budgeting Testing Officer - Commercial Banking (Independent) to join our team in Charlotte, NC. The role will be responsible for designing, implementing, and maintaining GRC solutions for our clients. The role will also be responsible for providing technical support to our clients and for managing the GRC solutions architecture.

Jobs Date Posted Experience Level Company Job Type On-site/Remote

Ethics & Compliance Controlling Manager - North America
Nike
Beaverton, OR
A minimum of 5+ years of experience in risk management, accounting, auditing or related functions
Experience within a large, multi-national company and CRCMP, CFE or other certification preferred
Solid understanding of the technical aspects of the Control Practices Act, as well as local Anti-Bribery laws and regulations
In-depth understanding of crafting and implement while also possessing a strong documentation skills
Understanding of internal auditing standards, CO Control Framework, and risk assessment practices
Experience in planning, implementing and report assessment results

Senior Compliance Project Manager
Dice
United States (Remote)
1 week ago · 8 applicants

Compliance and Quality Improvement Specialist
The University of North Carolina System
Chapel Hill, NC 27515
Remote

Info Security Advisor I - 100% REMOTE Opportunity
USA
Remote, TX
Possess (in good standing) security-related professional designation (e.g. CISSP, CISA, CRISC, CISM, etc.)
The above description reflects the details considered necessary to describe the principal functions of the job and should not be construed as a detailed description of all the work requirements that may be performed in the job.

Senior Audit Specialist, Global Risk & Assurance
SAP
New York, NY
SAP is looking for a Senior Audit Specialist, Global Risk & Assurance to join our team in New York, NY. The role will be responsible for designing, implementing, and maintaining GRC solutions for our clients. The role will also be responsible for providing technical support to our clients and for managing the GRC solutions architecture.

Director - PCI Compliance
Lexipol, Inc.
Las Vegas, NV 89109
• BBA or Master's Degree in MIS, Computer Information Systems or Other Security AND/OR professional designations in CISSP, CISA, CRISC, or CRCMP preferred.
• Must be able to create and maintain a Nevada Gaming Control Board Registration and certification or license, as required by law on a yearly basis.
• 10 years of work experience in Information Technology or related discipline.
• 5 years of work experience in banking with a national corporate government.
• Advanced knowledge in risk control, audits, process and access controls.
• 5 years of facilitating risk assessment sessions with all levels of management and executive management.
• 10 years of working risk assessment with all levels of management preferred.

Validated Certifications & Training

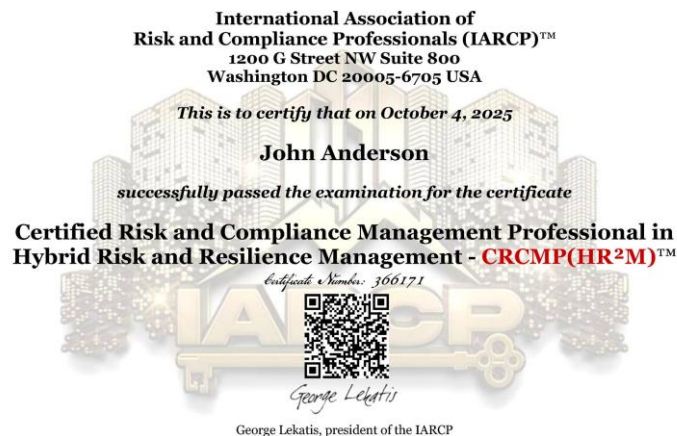
- Risk Management Professional (RMP)
- Certified Risk and Compliance Management Professional (CRCMP)
- Financial Risk Manager (FRM)
- Certified Accountant (CA)
- Certified Public Accountant (CPA)
- Certified Internal Auditor (CIA)
- Certified Information Systems Auditor (CISA)
- Project Management Professional (PMP)

We are SAP

2. Advanced Specialization, Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_HR2M.htm

The CRCMP(HR²M) program is designed to extend the capabilities of CRCMPs into the advanced domains of hybrid risk and resilience. This advanced specialization:

1. Moves from traditional risk and compliance frameworks into the management of multi-vector, cross-domain, and asymmetric threats that transcend conventional boundaries.
2. Develops expertise in hybrid risk governance.
3. Equips with the skills to design cross-sector resilience strategies, integrate governance across silos, and align risk frameworks with organizational, regulatory, and geopolitical realities.
4. Provides practical methodologies for hybrid stress testing, assisting organizations to withstand hybrid risks.
5. Advances the careers of CRCMPs by adding specialized expertise in hybrid risk and resilience, and offering strategic, cross-sector perspectives that are highly valued by organizations and boards.



Enrollment in the CRCMP(HR²M) program is restricted to professionals who have already passed the Certified Risk and Compliance Management Professional (CRCMP) exam.

To preserve the credibility and value of this credential, the association does not allow substitutions, equivalency credits, or waivers of any kind. The curriculum assumes mastery of the CRCMP body of knowledge.

3. Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program.

You may visit:

https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program

Overview

One of the most common (and costly) mistakes organizations make in the areas of risk management, compliance, IT, information security, and privacy, is relying solely on expert opinions that are **not grounded** in relevant laws and regulations. While professional expertise and technical insight are essential, they must be aligned with the legal and regulatory frameworks that govern these domains.

Without this alignment, organizations risk exposure to significant legal, financial, and reputational damage. For example, implementing information security controls based only on best practices, without accounting for legal requirements, can leave critical compliance gaps. Using risk management frameworks without tailoring them to specific regulatory requirements leaves organizations exposed to risk and compliance challenges.

4. Certified Cyber (Governance Risk and Compliance) Professional CC(GRC)P, distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program

Overview

There are still companies and organisations that consider cyber risk a technical risk. But even the most advanced organizations must adapt and build their risk management framework on the foundation that we now operate in a fundamentally different world, one where cyber risk is a core component of hybrid risk. The old mindset is dangerously outdated. Today, cyber operations are embedded in economic warfare, political conflict, supply chain disruption, and military strategy. Cyber risk today is not just about protecting networks, it's about protecting societies from hybrid threats.

A hybrid risk management framework should identify primary cyber threats, map their cascading effects on financial, legal, and business operations, and develop cross-functional response strategies.

5. Certified Risk and Compliance Management Professional in Insurance and Reinsurance CRCMP(Re)I, distance learning and online certification program. You may visit: [https://www.risk-compliance-association.com/CRCMP Re I.htm](https://www.risk-compliance-association.com/CRCMP_Re_I.htm)

Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I, distance learning and online certification program

Overview

In the aftermath of the global financial crisis of 2007–2009, and more recently the COVID-19 pandemic and the macroeconomic shocks triggered by inflation, geopolitical tensions, and climate-related events, the insurance and reinsurance sectors have faced escalating pressure to adapt to increasingly complex, interconnected, and systemic risks that challenge traditional risk models. These crises revealed not only the extraordinary complexity of risk exposures in the industry, but also the gaps in risk comprehension, governance, and compliance preparedness.

Mispriced risk, regulatory blind spots, and insufficient oversight contributed significantly to systemic instability. For insurers and reinsurers, the stakes remain immense. These firms serve as financial shock absorbers across society, and when their risk frameworks falter, the consequences ripple across markets, governments, and policyholders alike.

6. Travel Security Trained Professional (TSecTPro), distance learning and online certification program. You may visit: [https://www.risk-compliance-association.com/TSecTPro Distance Learning and Certification.htm](https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm)

Travel Security Trained Professional (TSecTPro), distance learning and online certification program

Overview

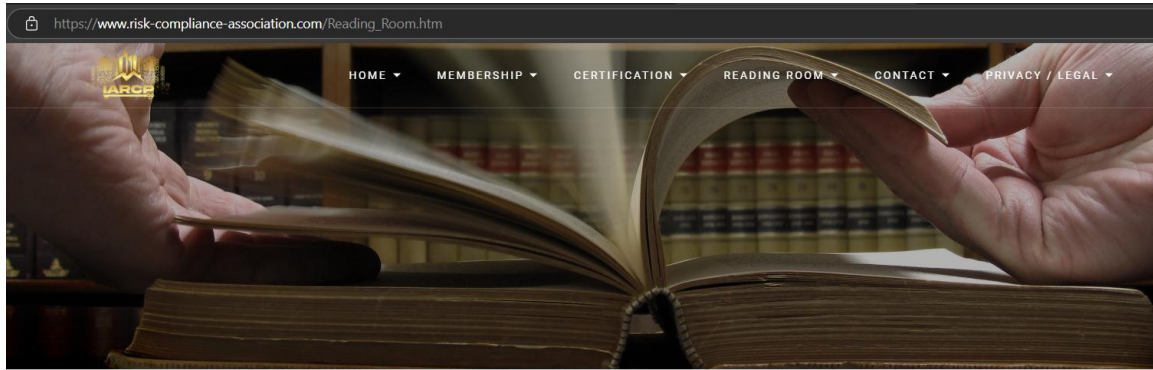
Professionals love international travel. For so many board members, senior executives, managers and employees, business travel taken for work purposes is also an opportunity for pleasure and satisfaction. It is about visiting new places, meeting new people, eating delicious food, having fun. For many, emotional or physical intimate relationships play a central role in the overall travel experience.

Intimacy refers to the closeness and connection – from intellectual intimacy (sharing thoughts, ideas, and professional experience) to emotional and sexual intimacy.

Travelers hate to think that travel also means increased risk, health challenges, legal uncertainty, and new unique threats. They often do not understand (or prefer to ignore) what it means to become subjects to the laws and the legal system of the countries they are visiting.

Our reading room:

https://www.risk-compliance-association.com/Reading_Room.htm



Reading Room, International Association of Risk and Compliance Professionals (IARCP)

Welcome to the Top 10 risk and compliance management news stories and world events that, for better or worse, defined this week's agenda – and a look ahead at what's coming next. This is the newsletter from the International Association of Risk and Compliance Professionals (IARCP).

You may contact:

Lyn Spooner

Email: lyn@risk-compliance-association.com

George Lekatis

President of the IARCP

1200 G Street NW, Suite 800

Washington, DC 20005, USA

Tel: (202) 449-9750

Email: lekatis@risk-compliance-association.com

Web: www.risk-compliance-association.com

HQ: 1220 N. Market Street Suite 804,

Wilmington, DE 19801, USA

Tel: (302) 342-8828

